Available online at: http://jurnal.president.university.ac.id

PROBLEMATIKA HUKUM

| ISSN (Print) 2477-1198 | ISSN (Online) 2503-4812 |

PRIVACY PROTECTION AND THE USE OF FACIAL RECOGNITION TECHNOLOGY IN PUBLIC SURVEILLANCE: LEGAL PERSPECTIVES AND POLICY IMPLEMENTATION IN THE DIGITAL ERA

Yonatan Kornelius Simanjuntak[1], Daffa Triakhsan Putra[2], Gragela L. Panjaitan[3], Christopher Geraldo Siregar[4], Natasya Sabatini Putri Pangaribuan[5]

[1]*Faculty of Law, President University, Indonesia. E-mail: yonatan.simanjuntak@student.president.ac.id*

[2]*Faculty of Law, President University, Indonesia. E-mail: daffa.putra@student.president.ac.id*

[3]*Faculty of Law, President University, Indonesia. E-mail: gragela.panjaitan@student.president.ac.id*

[4]*Faculty of Law, President University, Indonesia. E-mail: christopher.siregar@student.president.ac.id*

[5]*Faculty of Law, President University, Indonesia. E-mail: natasya.pangaribuan@student.president.ac.id*

Article

Keywords:

Artificial Technology; Facial Recognition Technology; Human Rights; Information and TechnologyLaw

Article History

Received: Apr.9,2023;
Reviewed: Apr.11,2023;
Accepted: May.15,2023;
Published: Jun.10, 2023

Abstract

The rapid development of facial recognition technology through artificial intelligence has raised various issues related to privacy and human rights. This is because this technology opens up the potential for abuse and violations related to this matter. In Indonesia, there are several regulations and laws that apply regarding information and technology and data privacy. Such as Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law), Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law), Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions, Law Number 24 of 2013 concerning Population Administration (Population Administration Law), Law Number 27 of 2022. Of course, there will continue to be challenges in dealing with the impact of facial recognition technology on society and the government. Therefore, it is very important for the public to learn about technology and start being tech-savvy, and it is very important for the government to make specific regulations on facial recognition technology. In addition, agile governance structures are also needed to adapt to technological advancements, such as oversight mechanisms, audits, and public consultations. These measures are essential to manage risks and protect privacy and individual rights in the digital age.

1. INTRODUCTION

(Waelen, 2023) mentioned in his journal, that the facial recognition system is a person's identification system based on facial stature or a mixture of composition of age, gender, race or other subjective sides in a person[1].

The use of facial recognition technology in public surveillance has become an increasingly hot topic of discussion around the world. As technology advances, the use of facial recognition technology by authorities raises questions related to privacy and human rights. In today's digital age, privacy protection is becoming increasingly important as the use of such technology becomesmore widespread.

Face recognition technology encompasses rapid developments in the fields of artificial intelligence and digital image processing. The origin of facial recognition technology lies at the intersection of artificial intelligence and digital image processing, where advances in machine learning algorithms have facilitated the development of advanced systems capable of identifying individuals based on unique facial features. This technology enables the identification of individuals based on their unique facial traits, such as face shape, eye structure, and distribution of other features. The success of this technology in public surveillance has also been demonstratedthrough its implementation in various scenarios, ranging from airport security to trafficmonitoringin major cities.

However, despite its obvious benefits in enhancing public security and surveillance, the use of facial recognition technology also raises serious concerns related to individual privacy. The identification of individuals through facial recognition technology has a significant impact on individual privacy rights and freedoms. With its ability to collect, store, and analyze biometric data, this technology opens up the potential for abuse and violation of human rights.

In recent years, the development of facial recognition technology has penetrated into various aspects of modern society, showing both admiration for its potential and concern over its implications. As the technology continues to develop at an unprecedented pace, the utilization of facial recognition technology in public surveillance has emerged as a controversial issue, sparking debates around privacy, human rights, and ethical considerations.

In terms of legal aspects, the main challenge is to harmonize the need to enhance public safety with the protection of individual privacy. Some countries have implemented regulatory frameworks governing the use of facial recognition technology, but there are still different

[1] Waelen, Rosalie A. *"The struggle for recognition in the age of facial recognition technology".* (December 2021)

approaches in addressing the related legal issues. Therefore, it is important to explore the legal aspects related to privacy protection and the use of facial recognition technology in public surveillance.

In response to these challenges, governments and regulatory bodies around the world have endeavoured to address the complex challenges of privacy protection and technological advancement. Legislative measures, such as the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), seek to establish a comprehensive framework for data privacy and regulate the use of biometric information. However, the effectiveness and enforceability of such regulations is still the subject of research and debate.

In the Indonesian context, the technological landscape of privacy protection and facial recognition is characterised by a mosaic of laws, regulations, and societal norms. The Electronic Information and Transaction Law (UU ITE), passed in 2008, provides a foundation for safeguarding privacy in the digital world, albeit with limited provisions specifically addressing facial recognition technology. Subsequent amendments and regulations sought to strengthen the existing legal framework, but gaps remain in addressing the unique challenges posed by facial recognition technology.

Against this backdrop, the importance of interdisciplinary research and collaboration becomes increasingly clear. Academics, policymakers, and stakeholders must collectively grapplewith the ethical, legal, and social implications of facial recognition technology, seeking to strike abalance between the importance of security and individual freedoms.

This research aims to investigate the legal implications of using facial recognition technology in the context of public surveillance. By considering the existing legal framework as well as policy implementation in various countries, this research aims to provide a deeper understanding of the challenges and solutions in addressing privacy issues in today's digital age.

This research seeks to explore the multifaceted dimensions of facial recognition technology in the context of public surveillance, with a particular focus on the legal implications and policy implementation in Indonesia. By examining existing legal frameworks, analyzing case studies, andengaging with related scholarly discourses, this study seeks to shed light on the complexities inherent in reconciling technological innovation with privacy protection.

In this introduction, we will discuss the background of the issues behind this research, explain the objectives of the research, outline the relevance of this research to the field of law, and summarize the structure of this journal article. In the next section of the article, we will embark on a comprehensive exploration of the issues surrounding facial recognition technology, covering legal considerations, social implications, and policy recommendations. Through careful analysis and critical enquiry, we aim to make a meaningful contribution to the ongoing discourse on privacyprotection and technology governance in the digital age.

As such, it is hoped that this article will make a valuable contribution to understanding issues relating to privacy protection and the use of facial recognition technology in public surveillance.

2. RESEARCH METHODOLOGY

This research methodology uses qualitative research methods as the main review in finding materials used for this research and to get answers to questions in the problem formulation. This research will refer to trusted and accredited journals, laws and regulations in Indonesia governing privacy protection and the use of facial recognition technology in public surveillance, and also websites that discuss this research. Then we will analyze the journals that we searched, analyze the laws and regulations that we obtained, and analyze the websites that we obtained. This analysis iscarried out in order to help the community in implementing existing policies so that existing policies can be implemented properly and optimally.

3. DISCUSSION

3.1 Problems that occured in the field of facial recognition technology

(William et al., 2023) mentioned that facial recognition technology is the process of identifying faces through a series of processes to obtain validation sourced from database assisted by artificial intelligence[2]. Facial recognition technology in the modern era is certainly a natural thing and is very often done to facilitate human life. But it turns out that behind this convenience there are several irregularities and loopholes for criminal aspects and the dissemination of personal data. Cases that occur often involve privacy or personal data of a person. Where in this modern era facial recognition systems are not only used by the government, but also many levels of society and companies where it can cause a lot of controversy.

A case that has occurred in Indonesia due to the use of facial recognition is one of the cases of the mobbing of Ade Armando by Abdul Manaf during a demonstration in front of theIndonesian House of Representatives (DPR RI) building in 2022. On one of the online news portals, kompas.com mentioned that initially Abdul Manaf was detected by the Indonesian

[2] William Charles, Wilson Kenny, Syahputra Bayu, Pratama Jimmy. "*Penerapan Teknologi Terbarukan dalam Bidang IT Pada Dunia Bisnis dan Masyarakat Implementasi A.I Face Recognition Thermal*". (November 2023)

Police facial recognition system. however, after tracing, the man named Abdul Manaf was detected in the Karawang area and was not at the crime scene. The reason given by the police is the level of accuracy of the technology they have in detecting faces[3]. Beyond this case, we must also find many AI systems that combine facial and voice recognition to create content. Where through this people's privacy can be disturbed because their faces and voices can be used without their permission and misused by others

Through this fact, we can find out how much the use of facial recognition systems is if used by irresponsible people. For example, there are private companies that use the technologyto cheat against their sector business rivals, or civilians who use the technology to facilitate crime. Of course, this can cause a lot of harm to society. The government in this case needs toimplement good and correct regulations and be implemented properly so that Indonesian citizens are protected from privacy or material losses by irresponsible parties and to reduce thenumber of new problems caused by AI technology which has been a problem that is very difficult to avoid.

3.2 Applicable laws on technology and data privacy in Indonesia

Based on the case that occurred and has been discussed before, of course we need to know what regulations and laws apply in Indonesia regarding information and technology and data privacy. Here are some applicable laws and regulations:

1) Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law). Although it does not specifically regulate facial recognition systems, this law regulates privacy protection in the context of the use of information technology.
2) Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE Law). This law further regulates data privacy while revising the previous law
3) Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions. This regulation regulates in detail the operation of systems, electronic transactions, service provider requirements as well as data protection and cybersecurity
4) Law Number 24 of 2013 concerning Population Administration (Administrative Law). Regulate population administration, including the use of public privacy

[3] Lely Maulida, Wahyunanda Kusuma Pertiwi. *Salah Tangkap Abdul Manaf Gara-gara Face Recognition, IniDeretan Kasus Serupa. Kompas.com. 14 April 2022*

data. So we can consider privacy aspects in carrying out activities using atechnology including facial recognition system technology.

1) Law Number 27 of 2022 About Personal Data Protection

   Facial recognition technology is one aspect of biometric data that the Journal says from(Rian Mangapul Sirait, 2023). What is further discussed in that journal is about regulations thathave not discussed specific matters related to procedures for applying for compensation, rightsin processing personal data and data protection implementing agencies. And based on the discussion above, facial recognition systems also include things that have not been specifically regulated in the laws and regulations in Indonesia. Where this should have been regulated considering the increasingly rapid development of technology and the destructive threat to society is certainly getting bigger.

3.3 Challenges for communities and government in dealing with the impact of facial recognition technology

(Umaroh, 2023) mentioned in the journal that AI has a role in many aspects of human life, this intersection makes there are ethical and legal implications that need to be taken into account in depth. Problems will arise in algorithms and databases that can sometimes make mistakes and cause fatal problems such as slander and defamation. Through the cases discussed, it has illustrated that the problems caused are very serious. Based on this, of course,the community and the government must take action to prevent and overcome the problems that will occur.

For people, it would be nice to learn about technology and start being literate about it. Where this is the basis for attitudes and actions that can be done to prevent losses caused by artificial intelligence (in this case the use of facial recognition systems). In addition, people must be more careful in providing personal data and using technology. However, if something that has the potential to be detrimental has happened, there is nothing wrong with immediately taking legal action against the relevant institution.

For the government, it will indeed be heavier in this regard. Many regulations must bemade or specific about facial recognition technology. Because its use will be more massive among the community, whether it's in the government sector or the private sector. Apart from regulations and laws, the government must also be swift and responsive to applicable law enforcement. Because the crime and problems caused will also run quickly. And the government becomes the most decisive sector in this regard. Where all levels of society or organizations depend on the policies made by the government.

4. CONCLUSION

Facial recognition technology, while offering undeniable conveniences, poses intricate challenges and substantial risks, particularly concerning privacy and data protection. The case of Ade Armando's mobbing by Abdul Manaf exemplifies the potential for misuse and errors inherent in facial recognition systems[4]. To address these multifaceted issues, Indonesia requires comprehensive and specific regulations tailored to the unique challenges posed by facial recognition technology.

While existing laws such as the ITE Law and Government Regulation Number 71 of 2019 provide a foundational framework, they do not directly or comprehensively address the intricacies of facial recognition technology. The recent enactment of Law Number 27 of 2022 on Personal Data Protection represents a progressive step forward. However, this law lacks specific provisions that directly address biometric data, including facial recognition. Therefore, further regulatory frameworks are imperative to ensure the responsible and ethical use of facial recognition technology, safeguarding individuals' privacy and rights in the digital age.

The complexities of facial recognition technology necessitate both proactive measures and adaptive strategies from both individuals and the government. Individuals must educate themselves to enhance their technological literacy, enabling them to understand and mitigate potential risks. Additionally, individuals should exercise caution when sharing personal data and utilizing technology. In the event of potential harm, individuals should be empowered to take legal action against relevant institutions.

For the governments, the challenges are even more serious. A robust regulatory framework specific to facial recognition technology needs to be developed in a timely manner. As technology becomes more pervasive in both the public and private sectors, regulation must remain flexible and responsive to ensure effective enforcement. Timely and responsive law enforcement is critical as rapid advances in technology require rapid adaptation to address potential crimes and challenges.

In conclusion, regulating facial recognition technology in Indonesia requires a comprehensive approach. This includes establishing a clear legal framework to define its permissible uses and guidelines for implementation, ensuring data protection, consent requirements, transparency, accountability, and mechanisms for redress. Building technical capacity is also crucial, including training programs for law enforcement and developing

[4] CNN Indonesia, *"Salah Tangkap Polisi Gara-Gara Face Recognition di Kasus Ade Armando",* 15 April 2022

standards for its ethical deployment. Additionally, agile governance structures are needed to adapt to technological advancements, such as oversight mechanisms, audits, and public consultation. These measures are essential for managing risks and protecting individual privacy and rights in the digital age.

REFERNCES

Journal/Article

Rian Mangapul Sirait, R. F. G. C. D. Br. G. (2023). Tantangan Hukum Penggunaan Data Biometrik Dalam Keperluan Bisnis.

Umaroh, A. (2023). Pertumbuhan Artificial Intelegence Serta Implikasinya Terhadap Hukum Dan Etika Ham (Salah Tangkap Pelaku Kriminal Menggunakan Teknologi Face Recognition). 1(3), 262–273. https://doi.org/10.59581/deposisi.v1i3.1082

William, C., Wilson, K., Syahputra, B., Pratama, J., & Gajah Mada Baloi Sei Ladi Batam, J. (2023). Penerapan Teknologi Terbarukan dalam Bidang IT Pada Dunia Bisnis dan Masyarakat Implementasi A.I Face Recognition Thermal. Journal of Information System andTechnology, 04(03), 431–434. https://doi.org/10.37253/joint.v4i3.6260

News

CNN Indonesia. (2022). Salah Tangkap Polisi Gara-Gara Face Recognition di Kasus Ade Armando. https://www.cnnindonesia.com/nasional/20220415075731-12-785112/salah-tangkap-polisi-gara-gara-face-recognition-di-kasus-ade-armando/amp